Appendix D
System Security Administration

Duties of the Security System Administrator (SSA)

The SSA must be extremely knowledgeable about the configuration of the system, the inherent security weaknesses in the use of the system components, and the security policy. To the extent that a potential threat could exploit the system, the SSAs must also remain current on vulnerability discoveries that may affect their system. The security aspects of the SSA's job are as important to the mission as the operation of the system. To that end, adequate resources must be available to allow SSAs to monitor any security policy violations and operational updates.

The SSAs must remain current in relevant technologies (e.g., operating system [OS], audit trails, configuration, and known vulnerabilities), and be provided an opportunity to remain current regarding potential attacks on their system. The System Administrator (SA) must keep the system running while the SSA ensures the Security Policy is upheld. If there is a security office for the information systems, then a SSA should be a member of that staff.

Under the direction of the Security Policy, the SSAs must operate and at times set up a secure system through use of mechanisms such as passwords (including provisions for protection, distribution, storage, length of character set, and valid duration period of password), security banners that cannot be altered by a user, session controls, lock screen, software and OS patches and updates, and account management. The SSAs must also remain current vis-à-vis potential weaknesses in the system by monitoring appropriate articles and Web sites, and they should also be on distribution for OS patches/releases and Computer Emergency Response Team (CERT) advisories. The SSA's responsibilities include conveying this information to the users, sending advisories, implementing patches, and updating procedures as needed to mitigate risk.

Configuration Management (CM)

There should be a CM Plan that includes a CM Control Board (with a security advocate); procedures for access and changes to hardware, software, and firmware; detailed and complete system diagrams; a complete map of the system, including which ports are available; how the computers in the system communicate with each other; a discussion on who has what privileges; virus protection; Internet downloading and personal software rules; software licensing agreements and procedures; a complete list of system resources (held by the SSA) and future requirements; upgrades planned, designed, and proposed; and movement of hardware. The SSAs must remain current on the configuration and is responsible for all upgrades and changes ensuring they do not violate the Security Policy.

Connectivity/Network Security

If the system is to be connected to other systems, the Security Policy must dictate the connectivity allowed. The SSAs must consider the countermeasures required to protect the information in residence or transit depending on said connectivity (e.g., Internet, dial-in, access gateways, remote access capable). When connecting to another system, it must be demonstrated that the local security policy will not be violated as a result of this connection.

Transmission

The Security Policy and the Security Features Users Guide (SFUG) should address how information may be transmitted to include security mechanisms required, the allowability of e-mail, specific protocols, and attachments, and specific security mechanisms such as the need for access control, possible access to the Internet and foreign nationals, the backbone over which the information will be transmitted, and the inherent vulnerabilities associated with use of the transmission media. The SSAs are responsible for providing this service while upholding the Security Policy.

Auditing and Intrusion Detection

The owner of the information must work with the SSAs to determine which events should be audited (should be determined by vulnerabilities applicable to the system). An audit trail must be maintained; an Audit Policy written as part of the Security Policy; an audit trail maintained (with Audit Reduction tools if needed), including any intrusion detection capability needed; and predefined procedures established to handle discovery of anomalous events. Audit data must be given special protection to prevent misrouting, modification, or deletion. Audit items must be updated as new vulnerabilities are discovered or when the security policy changes. The SSAs must enforce the Audit/Security Policy and monitor the audit trail taking appropriate action as defined in the Security Policy.

Labeling

The Security Policy must address labeling policies including what information should be labeled, and how and when it is to be labeled (e.g., transit, storage, on the screen, disk, hard copy, and e-mail attachments). The SSAs are responsible for ensuring all users are aware of these procedures.

Virus Protection

The Security Policy and SFUG should cover virus protection so that the users are familiar with the policy regarding the introduction of disks and software onto the system. The SSAs must make the SFUG available to all system users.

Backups

A backup procedure should be in place (documented in Security Policy), including information about types of backups performed and how often; where backups are stored; how often information is inventoried; and how it will be restored; and how the SSA will verify that the system security features are intact. Physical plant needs must also be addressed: is the room fireproof, what are the physical controls, is there an uninterruptible power supply (UPS), and are relevant items backed up and secured properly. The SSAs are responsible for ensuring all users are aware of these procedures.

Media Sanitization

The Security Policy and the SFUG should address how media are disposed of, (e.g., printed material, disks, and hard drives of sensitive and other information). The SSAs are responsible for ensuring that all users are aware of these procedures.

System Maintenance

The organization needs to determine how and when the system will be maintained. Areas to consider are whether remote maintenance is allowed, whether it is maintained in-house or by contractor, where maintenance diagnostics will be kept, and whether they are subject to configuration management. The concept of operations (CONOPS) (and parts of the Security Policy) should also detail the procedures for equipment repair (e.g., sensitive information should first be removed) and how and when both preventive and routine maintenance are performed. The SAs are responsible for system maintenance, as described in the CONOPS.

Physical Security

The Security Policy should document physical security requirements, including guards, alarms, locking procedures, badges, computer timeouts, exit inspection, cleaning service (escorted access and cleared access), and physical protection of the network. The SSAs are responsible for determining how the protection will be implemented (secure conduits and access to rooms).

Security Analysis of the System

A process must be defined to periodically assess the security posture of the system being protected. An independent group will assess the system for accreditation purposes. The SSA will ensure that the system meets the criteria specified by the accreditor, will explain the system to the assessment team, and will correct any problems discovered by the assessment team.

Suggested Documentation

- **Security Policy**—captures the security that is needed for a system supporting a particular mission and why that security is needed. It describes the mission that a system is intended to support, the mission goals, and information and resources important to the

mission. It identifies adversaries, their goals and motives (threat), impact statements (what is the damage if the policy is violated?), and the security policy guidelines (e.g., allowed connections). A range of security policies exists beginning at the national/departmental level going down through individual unit policies where refinement is made for local conditions.

- **CONOPS**—describes how the system will work, including connectivity and how information flows through the systems and to remote sites.
- **System Architecture Description**—describes in technical detail how the hardware and software provide the requisite security services.
- **System Configuration Management**—describes configuration data and the configuration management process.
- **Security Features Users Guide**—describes the security features and regulations for the system users.
- **Other Guides**—include a number of aides for system and security administration that were developed under the Secret and Below Interoperability (SABI) process and efforts to establish requirements for certification of security administrators that were completed recently.

The SSAs will need to be updated regularly; tailored information exists regarding the vulnerabilities and suspected or observed attacks on the network components, including internetwork infrastructure. This information would include items such as CERT advisories, vendor bug fixes, and articles about computer security bulletin boards.

References

Additional Information for SSAs

1. NCSC I942-TR-003 Version 1, Information System Security Policy Guidelines, July, 1994.
2. NCSC-TG-026, Version 1, Security Features Users Guide for Trusted Systems, September, 1991.
3. Frisch, Aeleen, Essential System Administration, 2nd edition, O'Reilly and Assoc., Sept, 1995, 101 Morris St, Sebastopol, CA 95472, (800) 998-9938.
4. Frisch, Aeleen, Essential Windows NT System Administration, O'Reilly and Assoc., Nov, 1997, 101 Morris St, Sebastopol, CA 95472, (800) 998-9938.
5. Garfinkel, Simson and Spafford, Gene, Practical UNIX and Internet Security, 2nd edition, O'Reilly and Assoc, July, 1991, 101 Morris St, Sebastopol, CA 95472, (800) 998-9938[6] Garfinkel, Simson and Spafford, Gene, Web Security and Commerce, June, 1997, O'Reilly and Assoc., 101 Morris St, Sebastopol, CA 95472, (800) 998-9938.
6. Nemeth, Eui, Snyder, Gart, Seebass, Scott, and Hein, Trent, UNIX System Administration Handbook, 2nd edition, Jan, 1995, Prentice Hall.
7. Russell, Deborah and Gangemi, G.T., Sr, Computer Security Basics, July, 1991, O'Reilly and Assoc., 101 Morris St, Sebastopol, CA 95472, (800) 998-9938.
8. Sutton, Steve, Windows NT Security Guide, Jan, 1997, Addison Wesley.

This page intentionally left blank.